UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

UNITED STATES OF AMERICA,	)
	)
Plaintiff,	) CASE NO. CR19-00159-RSL
	)
v.	) Seattle, Washington
	)
PAIGE A. THOMPSON,	) June 14, 2022
	) 9:05 a.m.
Defendant.	)
	) JURY TRIAL, Vol. 6 of 9

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE ROBERT S. LASNIK
UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the Plaintiff:

ANDREW C. FRIEDMAN
JESSICA M. MANCA
TANIA M. CULBERTSON
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101

For the Defendant:

MOHAMMAD ALI HAMOUDI
NANCY TENNEY
Federal Public Defender's Office
1601 5th Avenue, Suite 700
Seattle, WA 98101

BRIAN E. KLEIN
MELISSA A. MEISTER
Waymaker LLP
515 S Flower Street, Suite 3500
Los Angeles, CA 90071

Reported by:

Nancy L. Bauer, CRR, RPR
Marci Chatelain, CRR, RPR, RMP, CCR
Official Federal Court Reporter
700 Stewart Street, Suite 17205
Seattle, WA 98101
nancy_bauer@wawd.uscourts.gov

PROCEEDINGS

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE CLERK: United States District Court for the Western District of Washington is now in session, the Honorable Robert S. Lasnik presiding.

THE COURT: Good morning. Thank you. Please be seated.

THE CLERK: We are resuming our jury trial in the matter of the United States v. Paige Thompson, cause number CR19-159, assigned to this Court.

THE COURT: Okay. Somebody wanted to see me ahead of time; is that you, Mr. Hamoudi?

MR. HAMOUDI: Yes, Your Honor.

THE COURT: Okay.

MR. HAMOUDI: Thank you.

I just wanted some clarification regarding Agent Henderson's testimony.

Last night we received the exhibits that the agent intends to rely on. And the Court had said that he obviously cannot testify to her intent, but when the government asked whether he can look at certain like documents, like dark card -- carding forums dark web, and saying what is a carding forum dark web, the Court said it will allow that.

The exhibits that were provided to me last night are Ms. Thompson's Twitter messages. And my concern is this, that having the agent look at Twitter messages and being directly asked questions about Twitter messages is just another way of having Agent Henderson provide his qualifications and expertise to those messages. And what that will necessarily do is infer to the jury that -- on the ultimate issue in just another way. And we take the position that that violates Rule 704.

And separately, whatever probative value that process of questioning is is significantly outweighed by the danger of prejudicing her on this record.

He can certainly define those terms that are on those Twitter messages, and they can certainly during closing arguments say remember that term, bring up the Twitter messages, and argue to the jury, but on this record there is no evidence that she shared or monetized or did anything on these forums with this data. They spent three years looking at all of her records, all of her email accounts, and there's not a shred of evidence of that.

So I want to make that record and ask the Court that -- to not allow on those particular exhibits.

THE COURT: Well, I really have to see it in context. I can't tell you, no, don't show him Twitter messages, but I don't want him saying, yeah, this is exactly the kind of thing we see in identity theft or anything like that. But, you know, he can -- he can look at a tweet and say what that refers to is this or this.

And so it's -- we're going to have to do it on a question-by-question basis.

MR. HAMOUDI: And so then I ask for the -- for -- two things, that those exhibits not be published to the jury as he's making that comment, and he can use the document to provide that testimony, and then a limiting instruction, oral limiting instruction, consistent with Rule 704, be given to the jury after his testimony is received.

THE COURT: Well, do you have one for me?

MR. HAMOUDI: I can certainly prepare one right now.

THE COURT: We have enough lawyers in the courtroom, yeah.

MR. HAMOUDI: I can certainly prepare one.

THE COURT: Please.

MR. HAMOUDI: Thank you, Your Honor. I appreciate it.

THE COURT: And in terms of not showing him the exhibits that have been admitted into evidence, I'm not going to restrict the government in that area.

MR. HAMOUDI: Thank you, Your Honor.

THE COURT: Okay.

MR. FRIEDMAN: And, Your Honor, for the record, that's -- the way the Court has outlined it is what the government intends to do. And I expect we will oppose any limiting instruction that's proposed.

THE COURT: You will oppose?

MR. FRIEDMAN: I expect we will oppose whatever limiting instruction the defense may come up with, but obviously --

THE COURT: Okay. Yeah. That's fine, yeah.

So anything else before we bring the jury in?

Okay.

MR. FRIEDMAN: Yeah, nothing yet. We may ask for time at the break to speak about several issues.

THE COURT: Sure. Okay.

MR. FRIEDMAN: Thank you.

THE COURT: All right, Victoria.

Mr. Hamoudi, Colin Fieman was here for like five minutes; is he coming back at all?

MR. HAMOUDI: To the courtroom?

THE COURT: Yeah. Not today, but he was here a couple of days ago, I think.

MR. HAMOUDI: Yeah. I'm hoping he comes and watches me.

THE COURT: Yeah. Because then I could introduce Nick Brown and Colin Fieman.

MR. HAMOUDI: Mr. Brown is here.

THE COURT: Yeah. I don't want to just introduce the United States Attorney. But have him come in sometime.

MR. HAMOUDI: I will. I'll send him a message, Your Honor.

THE COURT: He may be a little busier than the U.S. Attorney, is that what you're saying?

MR. HAMOUDI: Well, he's trying -- he's trying to get his footing, and he's doing a very good job at it.

And we're short-staffed, Your Honor.

THE COURT: No, don't tell me that.

MR. HAMOUDI: Yeah. We're trying to hire a couple -- two or three lawyers right now.

THE COURT: Yeah. Okay. You know, I described for my wife the number of federal defenders who had been in the courtroom. And she's like, don't they have other cases to do?

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Good morning. Thank you. Please be seated.

Victoria, what a fabulous jury. They're always on time. They're always together.

THE CLERK: Yeah.

THE COURT: Really great. Thank you so much.

All right. Mr. Friedman, the next witness, please.

MR. FRIEDMAN: Your Honor, the government calls Kenneth Henderson.

THE COURT: Mr. Henderson, please raise your right hand and listen to the oath.

KENNETH HENDERSON,
having been first duly sworn, testified as follows:

THE CLERK: Would you please state your first and last names, and spell your last name for the record?

THE WITNESS: Sure. It's Kenneth Henderson, H-e-n-d-e-r-s-o-n.

THE COURT: Thank you.

You may proceed, Mr. Friedman.

MR. FRIEDMAN: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. FRIEDMAN:

Q. Good morning, Special Agent Henderson.

Where do you work?

A. I'm actually -- I work for the Secret Service based out of Washington, D.C.

Q. Okay. And you're a special agent there?

A. Yes.

Q. In general terms, what does a special agent do?

A. So Secret Service actually has a dual mission, so half of it is criminal investigations where we investigate fraud against the financial system, the other half is what you probably see on TV, protecting the president, vice president of the United States, among others.

Q. I'm sorry, at the end you said you're on the?

A. Among others.

Q. Among others, got it.

When did you become a Secret Service agent?

A. I was hired in 2015 and graduated from the academy early 2016.

Q. Where did you start out working as an agent?

A. I started in our Los Angeles field office.

Q. Okay. And did you have a particular assignment there?

A. Yes. I was assigned to our financial fraud task force.

Q. Okay. Did you invest credit card fraud -- investigate credit card fraud, among other things?

A. Yes.

Q. Did you work on a couple big cases involving credit card fraud?

A. I did.

Q. Can you tell us, in general terms, what was the first case?

A. Sure. The first case was an organized crime group that had multiple facets, the first facet being that they installed skimmers in the gas pumps.

Q. What's a skimmer?

A. So it's a little electronic device that actually goes inside the gas pump so a customer can't see it. And it records your credit card number as you dip it into the pump to pay for gas.

Q. And what did this group do after installing the skimmers?

A. So they collected the cards and made counterfeit credit cards with those numbers that they stole to steal gasoline from different gas stations around the area.

Q. Okay. A gas tank at a time?

A. Yeah. So they actually put it into a converted pickup truck that had a 400-gallon tank in the back so they could hold a lot of gas.

Q. And what did they do with the gas once they had purchased it?

A. Once they purchased it, they dumped it into a big tanker, like what you would normally see filling up a gas station, and they actually then sold it back to the gas stations for a reduced cost, but pure profit for them.

Q. And I used the word "purchased," that's probably not the right word for how they acquired that gas.

A. Right; the gas station purchased it from the bad guys.

Q. Okay. What was the second major case you worked on in Los Angeles?

A. Sure. It was another counterfeit credit card ring, but they basically -- the suspects had figured out that there was a foreign bank, actually it was a bank based in the Philippines, that lacked certain security controls. And they were able to guess credit card numbers using an algorithm for that bank.

Q. And when they guessed those credit card numbers, what did they do?

A. They made counterfeit credit cards and then they went and either purchased goods or purchased gift cards that they could sell for cash.

Q. Okay. How long did you stay in Los Angeles?

A. I was there for three years.

Q. So 'til 2019?

A. Correct, February of 2019.

Q. And where did you go in 2019?

A. I was transferred to our cyber intelligence section in our headquarters in Washington, D.C.

Q. And what does your cyber intelligence section do?

A. We investigate high-level cyber criminals, most of 'em Russian-speaking individuals, that hack and infiltrate the U.S. financial system.

Q. Okay. Do you investigate people who participate in, or, actually, carding forums?

A. Yes.

Q. What's a carding forum, in very general terms?

A. It's basically a website that these individuals log in, make an account, and where they basically meet and -- to exchange tips, talk about issues that they might be having, and also to buy and sell their goods, whether that be stolen credit cards or the malware used to steal those credit cards.

Q. Okay. And why is it called a carding forum?

A. So carding is basically shorthand for credit card fraud, so it's basically a credit card fraud forum.

Q. Has that been the focus of your work for the last three to four years?

A. Yes.

Q. Agent Henderson, I want to ask you some questions about, if a person had a large collection of PII -- are you familiar with the term "PII"?

A. Yes, personal identifiable information.

Q. Okay.

A. So your -- anything from Social Security numbers to email addresses, anything that can be used to identify you as a person.

Q. Okay. If a person had a large collection of PII, names, dates, Social Security numbers, how could -- what could the person do with that to monetize that collection?

A. Yeah. So there's a couple different ways, the first being just basically selling that whole data set to another individual. So, basically --

Q. Can I slow you up before you talk about that?

A. Absolutely.

Q. Are there ways the person could use that information themselves?

A. Yes. So they could actually create a website and -- much like there's many other websites on the Internet and the dark web, but they would basically sell to an individual customer at the end. Say that person wants to commit fraud, they want to buy five Social Security numbers --

Q. And, Special Agent Henderson, I'm going to take you even further back.

A. Yes. Sorry.

Q. Without selling to somebody else, without selling it on the Internet, are there ways people could use that information themselves?

A. Yes. So you could actually use that information to open up accounts for yourself, so you actually are the one committing the fraud. So if you have everybody's -- if you have someone's information, you could apply for a bank account, you could apply for a credit card. And since you have all of their identifiable information, the bank would not be aware that someone else is doing it in your name.

THE COURT: You used the phrase "the dark web."

THE WITNESS: Yes.

THE COURT: And could you describe what the dark web is?

THE WITNESS: Sure. So the dark -- the dark web is basically part of the Internet that you can't access via normal routes. So you can't go do a Google Search for something on the dark web, you actually would have to have a special browser, it's called The Onion Router, or otherwise known as the TOR browser for short. It sounds complicated, but anybody can download it. The only real hitch is that to get to a website, you need a very long URL. So instead of typing in Google.com, it's going to be a lot of letters and numbers, and end with dot onion, so...

THE COURT: Okay. Thank you.

THE WITNESS: Thank you.

Q. (By Mr. Friedman) So, Special Agent Henderson, you said one way the person could use that information themselves would be just to apply for credit cards with that information?

A. Yeah. If you have anything you need for a credit card application or a bank application, you could just fill out -- fill out the form and submit it and -- with your address, and receive the cards themselves, and start committing fraud.

Q. Okay. Could they also do something like the -- one of the cases you described before involving the Philippine bank?

A. Yeah. So there's basically an algorithm that is used to generate card numbers. There's usually lots of additional security steps that banks put on, but we have seen that some foreign banks overseas, banks lack those security controls, so you can actually generate a card number for use.

Q. Okay. For a foreign bank and you would then have a card -- a valid card number -- or valid -- you would have a card number that worked?

A. Correct.

Q. Okay. And then you were starting to talk about ways that the person could sell or transfer that information to others; is that correct?

A. Yes.

Q. What was the first way a person could do that?

A. So you could sell it wholesale. Basically, you have an entire database, you basically would advertise for sale on one of these carding forums, spell out what you have: Basically I have 50 million records that contain names, date of births, Social Security numbers, and then you would list a price. Usually, these sites actually are like eBay and it's like an auction site, so you usually name a starting price and how much a bid goes up or if somebody wants to buy it now and take all the bids off the table, you name a price for that as well.

Q. Okay. So that's one way you could sell this information.

Did you also mention another way or were you starting to mention a second way to do that?

A. Yeah. So the second way would be to create a site yourself, basically a place where somebody who wants to commit fraud would go, log in, and select a PII of someone to purchase, so an individual record. So those can span the spectrum from $1, 1.50, upwards of $20, depending on what kind of information is associated with that record.

Q. So if I know a site like that and I want to go there, I can buy basically a person's profile, their name, date of birth, Social Security number, the works?

A. Yeah. Yeah, and address, email, all of that with a click of a button.

Q. Okay. If a person had a large trove of information, PII, would it be helpful if you were trying to use it to sort that information?

A. Yes. Kind of two reasons to sort that information. First, to figure out what you have, right. It's a lot -- you'll get a higher purchase price if you're able to dictate to someone what exactly you possess, how many -- how many Social Security numbers, how many names, how many addresses. Somebody's willing to -- will pay more if you give them specifics, rather than generalities.

Q. And why does sorting that information make it easier to give those specifics?

A. Because you'll be able to basically sort all the data down and you can look at all the columns, just like a very large Excel document, and see how many records you actually have.

Q. You can count how many rows there are in the database?

A. Correct.

Q. Is it also useful to sort the information by name, date of birth, Social Security number, the other characteristics the information may have?

A. Yeah. Because each record's going to be different, maybe contain different information. So if you ever -- if you do want to create one of those sites, you basically would need everything very organized for a computer program to generate that -- to show on their website.

Q. How does that -- how would sorting data affect the value of that data?

A. It creases the cost, right. It's sometimes hard work, especially if we're talking about large amounts of data, to sort it. Sometimes you need a lot of computer processing power, you need special programs. So if it comes presorted, people will buy it at a premium price because they don't have to do that work themselves or find somebody to do that work.

Q. Okay. Is sorting by location particularly important?

A. Sorting by location can certainly help if you're committing fraud yourself, so lots of banks, especially U.S. banks, have fraud controls in place that focus on where the location is of the customer versus where the location is of where those either goods or services are being purchased. So they might raise a red flag if you are a customer based in Seattle but you're suddenly spending in South Dakota.

Q. Or applying for a credit card?

A. Or applying for a credit card.

Q. Okay. Have you reviewed some Google Search history in this case?

A. I have.

Q. Okay. And I'd like you to look at Exhibit 504, page 59.

Do you see a search at the top of that page?

A. I do.

Q. Okay. What was the search for?

A. "Carding forums dark web."

Q. You spoke a moment ago about the dark web.

A. Yes.

Q. What do you -- or do you have a word or is there a generally accepted word for what we all think of as the Internet?

A. Yeah. The clear web would be what we would be able to search for on Google.

Q. Okay. So if you go to Google and type a search in, it's searching sites on the clear web?

A. Correct.

Q. How would you find sites -- and so what's the difference between the clear web and the dark web?

A. So the difference being that you wouldn't be able to find one of these websites searching Google.

Q. So it's out there, but you can't find it?

A. Correct.

Q. Okay.

A. You would need a -- you need the specific website address to get to it.

Q. And if you have the address, you can go to it, even though you can't find it in a search?

A. Correct; with the special browser that you download called the TOR browser.

Q. The Onion Router browser?

A. Yes.

Q. Okay. Are there carding forums on the clear web?

A. There are.

Q. Are there also carding forums on the dark web?

A. Yeah. Most have a presence on both.

Q. Okay. And so what do you understand this search to be a search for?

A. So while it's hard to find those websites on the dark web, there are websites on the clear web that basically give you a directory, list those addresses that are hard to find for easier navigation.

So this search would clearly be looking for one of those sites that's a directory of those carding forums and their address -- associated address on the dark web.

Q. Okay. And once you obtain that address, what could you do?

A. Then you could access the carding forum via the Onion Browser.

Q. Okay. Let's go one page earlier, I think it's search 406, and tell me if you see what that is a search for.

MR. FRIEDMAN: Special Agent Martini -- there we go.

Q. (By Mr. Friedman) Could you look at the bottom two searches on this page?

A. Yes.

Q. When were these searches conducted?

A. They were conducted May 5th of 2019.

Q. Is that the same date as the other search we looked at a moment ago?

A. Yes.

Q. Okay. What is the first search for here?

A. Credit card numbers algorithm.

Q. Okay. You touched on this briefly, I think, but what is -- is there an algorithm that is related to credit cards?

A. Yes. So a credit card is a 16-digit number. The first six digits are what's called a bank identification number, it's -- basically, those six digits are assigned specifically to one bank. So a bank might have multiple of 'em, but only one bank uses that bank identification number or BIN. The rest of the numbers are generated with an algorithm, with that last digit being a check on the credit card number to make sure all the other ones are valid before it gets to that check number.

Q. Can you explain what you mean by a check? How does the last digit function as a check?

A. So it's basically a mathematical equation. You basically double all the numbers in -- on the credit card, you divide it by a certain amount, and it equals -- it will equal that check number at the end.

Q. Okay. And if the -- it's a pretty simple formula, right, just doubling the other digits?

A. Yeah. At the end of the day, it's a very simple algorithm, but it's been used since the invention of the credit card.

Q. But if they don't match the last digit, the whole card number doesn't work?

A. Correct; it's automatically rejected by the system.

Q. Okay. How is it helpful for someone who wants to commit credit card fraud to understand this algorithm?

A. So it narrows down the possibilities, possible card numbers, so you're not starting with 1, 2, 3, 4, 5, 6, 7, 8, 9. If you have that BIN, that first six digits, which you can easily also look up online, the rest is just an algorithm. And it narrows down the range of possibilities of active credit card numbers.

Q. Okay. And then do you see a search right -- I'm sorry, so would it make you more efficient?

A. Yes.

Q. Okay.

Fewer dead ends?

A. Correct.

Q. Do you see another search right above -- or right below this search?

A. Yes, "Top 5 Carding Forums."

Q. How many carding forums are there out there?

A. Quite a few. The ones -- ones that are good and trusted probably range in about those five.

Q. Okay. Are those carding forums generally located in particular places?

A. Yeah. So the servers themselves, obviously they know they're up to nefarious acts and would be looked at by law enforcement, so they keep the servers out of reach of western law enforcement. And they're usually based in countries that are not helpful with the United States, such as Russia, Iran, or other former eastern block countries.

Q. Okay. All of the searches that we've just looked at were conducted in early May, correct, May 5th?

A. Yes.

Q. Have you seen searches conducted about a month later?

A. I have.

MR. FRIEDMAN: And could we go to page 31 of this exhibit, Special Agent?

Q. (By Mr. Friedman) And -- okay. I'm not focusing on exactly the right search here. Do you see --

MR. FRIEDMAN: If we could look at the first couple searches.

There you go.

Q. (By Mr. Friedman) Yeah. What is search 203?

A. So the search is for "Planetahost Data center."

Q. Okay. What is that?

A. It's a data center located in Russia where you could host either data or websites.

MR. FRIEDMAN: Okay. And then if we go down to the very bottom search on this page, please?

Q. (By Mr. Friedman) What's that search for?

A. The last search is for "Server rental in Moscow/Planetahost."

Q. Okay. Would it be helpful for someone who was interested in selling credit card data to host that on a server somewhere?

A. Yes. It's easy to pass that information to other individuals without having them connect to your home computer.

Q. Okay. Why would it be helpful to do that in Moscow in particular?

A. Like I mentioned before, Russia is not friendly when it comes to these type of requests with -- from law enforcement, so it would -- the contents, or the customer records, all that information, would be out of reach of U.S. law enforcement.

Q. Are you aware of other reasons, apart from being outside of the reach of law enforcement, other advantages to renting a server and using a server in Moscow instead of somewhere else?

A. I'm not. Usually, these servers are slower speed and have less -- less technologically advanced than servers located elsewhere.

Q. Okay. Have you also looked at chats from about this same date?

A. I have.

Q. Okay. And would you look at Exhibit 455, page 2?

Is that an IRC chat that was actually sent on this very same date?

A. Yes.

Q. Okay. Could you -- starting at the second line, could you read that chat or that -- I guess the three lines that begin at the second line?

A. Sure. "I dunno my friend said something to me awhile back thats got me thinking about carding alot lately Luhn algorithm shit and other issuance characteristics."

Q. And what does carding mean to you?

A. Carding would be credit card fraud.

Q. The Luhn algorithm, is that the algorithm you were talking about earlier?

A. Yes.

So the Luhn algorithm is the algorithm used to generate credit card numbers.

Q. The next line refers to a mag track writer. What is a mag track writer?

A. So that black stripe on the back of your credit card is a magnetic stripe. So a mag track writer is used to encode that black stripe with your name, with the credit card number, so when you swipe it, it can pass that information along to the point of sale system.

Q. Okay. And then the line after that refers to something called an emboss kit?

A. Yes.

Q. Emboss kit, sorry.

What are emboss kits?

A. So otherwise known as an embosser. Basically, to prevent credit card -- counterfeit credit cards; and also, if everybody remembers the old machines used with carbon paper, those numbers on your credit card are raised up, so not just printed, but raised up. And so an embosser is used to make those raised numbers and, usually, name raised on the credit card.

Q. Okay. If --

THE COURT: I see all the heads in the jury box of people over 60 who are remembering those days, and the young people looking at us like, what are you talking about.

THE WITNESS: It was a good sound.

THE COURT: It was, yeah.

Q. (By Mr. Friedman) The Secret Service have some antiques in its headquarters in D.C.?

A. Yeah. There's a museum if everybody wants to come to in D.C.

Q. Are you familiar with something called white plastic?

A. Yes.

Q. What's white plastic?

A. So it's basically a credit-card-size piece of plastic with that magnetic stripe on the back. They're usually white, blank, so that's why they get their name, white plastic.

Q. Okay. And if you have white plastic, a mag track writer, and an emboss kit, what can you do?

A. You can make a counterfeit credit card.

Q. Okay. What about if you just have a gift card purchased from a store, like a supermarket coun- -- supermarket counter?

A. Yeah. If it has that mag stripe on the back, you can what we call re-encode, basically change what's encoded on that mag stripe, and use it as a credit card.

Q. So this was early June; is that correct?

A. Correct.

Q. Have you also looked at messages on Twitter from a month later, early July?

A. Yes.

MR. FRIEDMAN: Okay. Let's look at Exhibit 435, if we could?

And could we focus on the top message here?

Q. (By Mr. Friedman) Can you read that message?

A. Sure. "Im gonna give it to worse people too, im gonna give it to an avid scammer, a chinaman who will find a good perm home for it on the black market, sealed with a story behind it."

Q. Is trust something that means something to you in the world of credit card fraud?

A. Yeah. So the old saying, right, is no honor among thieves, but there is some trust built up if people have personal business relationships with other users on these forums.

Q. So if someone just -- if I just open an account on a forum and start advertising stuff, what's likely to happen?

A. People would not trust that what you have is the actual thing that you're advertising. If you have some more reputation behind you, if you've had some successful deals in the past, they're willing to do more business with you and probably give you money or give you a premium on that sale because they know it's legitimate.

Q. Okay. How does that affect how you interpret this message?

A. Well, clearly it appears that someone would probably --

MR. HAMOUDI: Objection, Your Honor.

THE COURT: I'm going to sustain the objection to this question.

Q. (By Mr. Friedman) Have you looked at web searches that took place at approximately that time?

A. I have.

MR. FRIEDMAN: And if we could go back to Exhibit 504, page 14.

Q. (By Mr. Friedman) Do you see -- these may not all be searches, but do you see a number of websites -- pages of websites visited here?

A. Yes.

Q. And for what are those pages?

A. So it's a product called Databricks that is a Microsoft product.

Q. What does Databricks do?

A. It's basically a cloud service that helps individuals or businesses organize a lot of data and basically process it into a more searchable, usable format.

Q. Okay. If you don't have a large amount of data, is there any particular way in which Databricks would be useful to you?

A. Not to my knowledge.

MR. FRIEDMAN: And then if we could turn to pages 10 and 11 of the same exhibit.

Q. (By Mr. Friedman) Do you see -- so we're at page 10. Do you see a search at the bottom of that page?

A. Yes.

Q. What is that a search for?

A. It appears to be a YouTube video focused on an embosser.

Q. Okay. What is an embosser?

A. So, again, it's that machine that's used to create those raised numbers and names on your credit card.

Q. Like a more formal name for an emboss kit?

A. Correct.

Q. Have you vis- -- have you looked at this video?

A. I have.

Q. And what does this video tell you or explain to you, teach you?

A. So it's basically a user that found a large-scale embosser in a dumpster. And he went through -- basically took it apart and showed what the individual parts did.

This one in particular printed on the card, it can emboss on the card, and also can record on that magnetic stripe information that you would want recorded on it.

MR. FRIEDMAN: Okay. And if we could go to the next page, page 11.

Q. (By Mr. Friedman) Do you see two searches or pages at the top of that page?

A. Yes.

Q. What do those refer to?

A. So that's the model -- the manufacturer and the model number of that embosser that was on the YouTube video.

Q. Are you generally familiar with that particular embosser?

A. Yes.

Q. How much would that one cost?

A. Upwards of $15,000.

Q. Okay. Have you also looked at -- so if this is early July, have you also looked at IRC chats from mid-July?

A. Yes.

Q. Okay. I'm going to ask you to look at Exhibit 459, page 2.

Is that the chat or one of the chats at which you looked?

A. Yes.

Q. Could you read the second line?

A. "Kongfuzi: you got a place to upload 2.2TB of stuff."

Q. Okay. And 2.2 terabytes, what does that mean to you?

A. It's a very large set of data.

Q. And what does upload mean?

A. Would be putting that data onto a server.

Q. Okay. And in credit card cases that you've investigated, is uploading data to a server necessary or part of those cases?

A. Yes.

Q. And why is that?

A. To pass that information along, it needs to be uploaded to a server where then somebody can obtain credentials and then download it themselves.

Q. Okay. You've looked at a certain amount of evidence in this case; correct?

A. Yes.

Q. Are you aware of any evidence that Ms. Thompson actually sold the information that was in her possession?

A. I did not see any evidence, no.

Q. Okay. This text -- this chat was July 14th; is that correct?

A. Yes.

Q. Are you aware of a spreadsheet that contains sorted information in this case?

A. Yes.

Q. And are you aware of the metadata relating to that spreadsheet?

A. Yes.

Q. When does it show that spreadsheet was last moved or --

A. Shortly after this chat.

Q. Still in July?

A. Yes.

Q. Okay. And are you aware when Ms. Thompson was arrested in this case?

A. Shortly after that, about two weeks later.

Q. Okay. Special Agent Henderson, have you attempted to analyze the value of the data taken from Capital One in this case?

A. Yes.

Q. Okay. And you're generally aware of what that data was; is that correct?

A. Correct.

MR. FRIEDMAN: If we -- could we look at Exhibit 715?

Q. (By Mr. Friedman) Do you understand that to be a summary of the number and types of records in the case?

A. Yes.

Q. Did you rely on that in attempting to analyze the value of this data?

A. I did.

Q. So how did you go about that?

A. I tried to find a data set that had been listed for sale of similar contents. The best analogy I could find was in August of 2021, a data set from T-Mobile was advertised on one of these forums for sale and listed the sale price at $275,000.

Q. Okay. And what, in general terms, was that data set?

A. So information hacked from T-Mobile. It contained names, dates of birth, Social Security numbers. It did not contain email addresses or anything about income.

Q. Okay. And I may have missed it, how many records were in that data set?

A. There was 30 million records in that data set.

Q. Okay. So based on that data point, what did you conclude about the value of this data set?

A. So this data set obviously is about three times larger than that one and doesn't include as many Social Security numbers, so I -- it certainly wouldn't fetch three times the price, but I would venture to say it would fetch around $500,000.

Q. Did you do the calculation sort of a different way to double-check or get a different possible value for part of this data set?

A. Yeah. So just strictly looking at the Social Security numbers, 117,000 Social Security numbers. There's websites that will sell you someone's Social Security number, probably my own, too, for about $1.50. So estimating some profit margin in there, I'd estimate that she could sell the Social Security numbers records for about $1 each, so that would be $117,000.

Q. For just the records with Social Security numbers?

A. Correct.

Q. Not the other 97 million records?

A. Correct.

Q. Based on those two analyses, do you have an estimate of the total value of this data sold on a carding forum or otherwise for fraudulent purposes?

A. Yeah. I'd estimate she'd be able to get upwards of $650,000.

Q. Do you have any doubt that the data was worth more than $5,000?

A. None at all.

MR. FRIEDMAN: May I have a moment, Your Honor?

THE COURT: Sure.

(Off the record.)

MR. FRIEDMAN: Thank you, Special Agent Henderson.

THE COURT: Okay. Mr. Hamoudi will have some questions for you now.

MR. HAMOUDI: Can I have a moment, Your Honor?

THE COURT: Sure.

(Off the record.)

THE COURT: Do you have any desire to go to the other side of the Secret Service and start protecting?

THE WITNESS: I'm very lucky, I'm one of the very few that doesn't have to do that full time, but everybody has to do it at least part-time.

THE COURT: Sometime.

THE WITNESS: Yes.

CROSS-EXAMINATION

BY MR. HAMOUDI:

Q. Good morning, Agent Henderson. Did you ever talk to Capital One regarding the data that was involved in this case?

A. I did not discuss this case with Capital One.

Q. Did you talk to individuals who actually analyzed the data?

A. No.

Q. Okay. And you spoke about the T-Mobile data?

A. Correct.

Q. How old was that data?

A. It was posted for sale in August 2021. It seemed to -- from news reports -- I'm not part of that investigation. From news reports, it was hacked shortly before.

Q. Okay. So -- but you never looked at the substance of the data, analyzed it, to determine how old it was; correct?

A. The T-Mobile data?

Q. Yeah.

A. Correct.

Q. And you don't know why any of these Internet searches were conducted; correct?

THE COURT: When you say "these," you mean the ones in Ms. Thompson's --

Q. (By Mr. Hamoudi) Yeah, the ones that you viewed, the web searches?

A. No.

Q. And to sort of follow up on that, it's not illegal to search the Internet; correct?

A. That's correct.

Q. I mean, people search the Internet and put in to the web browser all kinds of things; correct?

A. Sure.

Q. And if we were to examine, even yourself, the last two years of your web searches and selectively pull your web searches out, we could try to suggest things; correct?

A. I'm sure you could.

Q. Yeah.

And in this case, you have seen no evidence that Ms. Thompson applied for credit cards under a name other -- anybody else's name; correct?

A. Correct.

Q. Or that she created credit cards or bank accounts; correct?

A. Correct.

Q. Or sold or transferred any data to anyone else; correct?

A. Correct.

Q. And you spoke about the 2.2 terabytes of data that was in that message. Do you recall that?

A. Yes.

Q. How much was the content of the data belonging to Capital One? Do you know the answer to that question?

A. Not off the top of my head.

Q. Okay. And there's no evidence that you've seen that Ms. Thompson bought anyone's personal information; correct?

A. Correct.

MR. HAMOUDI: I don't have any other questions for the agent, Your Honor.

And I would ask -- I have a copy of the limiting instruction, if I could hand the government and the Court.

THE COURT: Sure. Go ahead.

MR. HAMOUDI: Okay.

May I approach, Your Honor?

THE COURT: Sure.

MR. HAMOUDI: I'm sorry, it's a little bit -- it's not typed. I wrote it out.

THE COURT: Okay. We -- you don't have any more questions for Agent Henderson?

MR. FRIEDMAN: I don't, Your Honor.

THE COURT: Okay. You may step down, Agent. Thank you so much for coming in.

THE WITNESS: Thank you, sir.

THE COURT: I'm not going to utilize this.

MR. HAMOUDI: Okay. Thank you, Your Honor.

THE COURT: Sure.

Next witness.

MS. MANCA: Thank you, Your Honor. The government calls John Strand.

THE COURT: Mr. Strand, come on up to the open area of the courtroom here, please.

That way, yeah.

Please raise your right hand.

JOHN STRAND,
having been first duly sworn, testified as follows:

THE CLERK: If you could please state your first and last names, and spell your last name for the record.

THE WITNESS: Yeah. My name is John Strand, S-t-r-a-n-d.

THE COURT: Thank you, Mr. Strand.

Go ahead, Ms. Manca.

MS. MANCA: Thank you.

DIRECT EXAMINATION

BY MS. MANCA:

Q. Good morning, sir. Where do you work or what do you do?

A. I'm the owner of Black Hills Information Security, penetration and testing security firm.

Q. When did you start Black Hills Information Security?

A. It was founded in 2008.

Q. How many employees do you have?

A. Right now we're about 100 employees.

Q. Where is the company headquartered?

A. We are headquartered in Deadwood, South Dakota.

Q. What do customers hire you to do?

A. Specifically, they hire us in a couple of different fashions. First one is to actually do security assessments and break into their organizations in the hopes of trying to remediate security vulnerabilities. And we also do security operation services where we work with organizations to help secure and lock down their environments as well.

Q. How did you become involved in cyber security or network security?

A. I got involved in computer security in the *Cobell v.* -- *Cobell v. Department of Interior* case while I was working at Eccentric Consulting back in 2000. Worked that class action lawsuit and helped secure their networks and mineral resources management for the United States government.

Q. At that time, did you have a degree in computer science or anything related to computers?

A. No. At that point, I did not. I actually had a political science degree.

Eventually, I ended up getting my master's degree from Denver University.

Q. What is your degree in?

A. Specifically in computer security.

Q. Do you give presentations on cyber security or network security issues?

A. Yes. We do regular web casts and webinars and just educational efforts for the community as a whole. We do, I think, three or four web casts a week that are free to the community, anywhere from vulnerability research, different ways of securing and locking down organizations.

I was also an instructor for an organization called the SANS Institute specifically in offensive security training. And SANS stands for Systems Administration Network Security. And they are the world's largest information security training organization.

Q. How long have you taught for SANS?

A. Actually taught with them for 17 years.

Q. What kind of people or organizations take classes at SANS?

A. A tremendously wide variety of people, anywhere from Department of Defense, cyber security operators, all the way to Fortune 100 companies, down to systems administrators that are trying to secure mom-and-pop, bicycle shops, things of that nature.

Q. What kind of classes do you teach at SANS, or did you teach at SANS?

A. Specifically the offensive classes. I wrote and taught classes. One of them was Hacker Techniques, Exploits, and Incident Handling. That was the main class that I taught at SANS. And I taught about a thousand people a year live for that class and a number of people online. They had on-demand training as well. So trained a large number of people with that class.

I've also taught other classes specifically for network penetration testing, advanced exploitation development, and also using specific tools that are used in the security community, tools like Metasploit is one of the tools that we used to use quite a bit back in the day.

Q. So in teaching what you're referring to as offensive techniques, I mean, you essentially teach hacking?

A. That's correct, absolutely. Specifically, teaching hacking for the purposes of trying to get organizations to do self-assessments so that they can secure their own organizations as well.

Q. Do you believe that hacking plays a role in making computer systems more secure?

A. Absolutely, without question.

Hacking and good-faith security research are absolutely critical. One of the analogies I like to use is architecture. You're in a building that has trusses, it has beams, it has columns. Everything in this building has a failure point where enough weight, enough shear will cause it to fail. The same thing is true in IT. Absolutely everything has failure points and it's up to us in the security community to help identify these failure points so that we can build better architectures, so that our IT architectures aren't susceptible to as many attacks.

Q. Are there limitations on good-faith security research?

A. Absolutely. Depends on specifically what the goals and objectives are.

If you're doing good-faith security research, your primary goal should be trying to either secure the organization or trying to help secure the entire community. That is your good-faith security research, you're reaching out, you're trying to make the industry better.

Q. What does it mean to help secure an organization or help secure the Internet as a whole?

A. So it basically means finding those weak points that exist in our architectures and our components. For example, if you had a vulnerability in something like, let's say, DNS, your computer doesn't know what Yahoo.com or Google.com is, it has to convert it into a number, which is a lot like a phone number. So if somebody could come up with a vulnerability, which has happened in the past that allows you to take over, you could reroute traffic anywhere you want. That would be a vulnerability that would impact the entire ecosystem of the Internet.

So security researchers will help find those types of vulnerabilities and then work with multiple companies to try to remediate those vulnerabilities so the overall architecture is stronger. That's a macro example.

On a micro example, it might be something as simple as finding a vulnerability in software we use every single day, and then helping the company remediate that vulnerability.

Q. What role does responsible disclosure to the vulnerable company or organization play in good-faith security research?

A. So whenever you're looking at vulnerabilities, vulnerabilities can originate in a variety of different ways. One of those ways is they can hire firms like Black Hills Information Security to test and identify those vulnerabilities. Other vulnerabilities may show up just from the day-to-day use of a product, of software online. So a customer could be using software from somebody, let's say like Microsoft, and find a vulnerability in that software. And then they would coordinate with that vendor to help remediate that vulnerability.

The other thing that you can see, and you can see quite often in the community today, is you have security researchers that are specifically looking for vulnerabilities in software.

In fact, there was one that was just released today that I was reading where somebody found a vulnerability in Microsoft Azure that allowed you to get data from multiple different customers. They spent four months working with Microsoft and eventually got paid for their efforts to fix that vulnerability.

Now, they were not originally hired by Microsoft to do that, they did that as part of their job, which is just general vulnerability research. But they coordinated that vulnerability, got it fixed with Microsoft, and eventually got paid for it as well.

Q. And the woman in front of you is a court reporter who is writing what you say, and so both you and I speak very quickly, so we're going to slow it down just a little bit, if that's all right.

A. Sounds fine.

Q. Okay. Is the goal of security to eliminate vulnerabilities?

A. That is one of the things that we do in security, but it is not the ultimate goal of computer security to remediate and remove all vulnerabilities. In fact, that's not possible. It's not an Easter egg hunt. You don't find all the vulnerabilities and then there are no more. If you look at software, it's constantly written by human beings, and we always make mistakes. So we're writing software all the time.

And also, there's this huge explosion of technologies. I'm sure you see cloud computing and things like that. That massive explosion of code leads to more and more vulnerabilities being introduced.

Further, we're also seeing software constantly being updated with more and more features that also introduces more vulnerabilities. So that's why it's important not just to be looking at vulnerabilities, but also looking at from the perspective of architecture, so if a vulnerability does arise, it doesn't lead to a catastrophic loss of life or tremendous amount of financial impact to people.

Q. Do you have a sense of how many potential vulnerabilities there are out there, or potential exploits?

A. Let's just say there's hundreds of thousands of vulnerabilities that are out there that are actually documented. There are hundreds of thousands of vulnerabilities since they started keeping record way back in the early 2000s.

Q. Does Black Hills Information Security do both offensive testing and threat mitigation or internal defensive work?

A. We do. We call that purple teaming. And let me explain the term.

A red team would be somebody who is doing something that's offensive. The terminology goes back to Department of Defense emulating what Russians would do.

Blue team would be the team that's doing defensive technologies. So we do a lot of work where we're doing offensive research on a company, and we're also working with the blue teamers to try to put in and mitigate security vulnerabilities; not just like an exploit per se, but overall architecture to make it more resilient to attacks.

Q. So how do red teams and blue teams work together?

A. One of the things I always like to say is we're all purple because if I'm a red teamer and I'm doing offensive stuff, I'm trying to emulate what an attacker does, but my goal is to make the defense better. So my goal in life and what we do every single day is to make my life harder. If my life gets harder, then your lives and everyone's in this room, we're more secure as a whole.

So with red team and blue team working together, we call it purple because, you know, the colors mix, but the goal is ultimately to make security better across the entire industry.

Q. Are you familiar with the term "white hat hacker"?

A. Yes, I am familiar with the term.

Q. What about "black hat hacker"?

A. Also familiar with that term as well.

Q. Is the technology industry trying to move away from that terminology?

A. Yeah. Generally, we're trying to get away from white hat and black hat, whitelisting, allow-listing, we're trying to get away from those terms and use things like allow list, deny list, or safe list. And when we are talking about vulnerability research, we're generally trying to move away from those terms as well.

Q. And that's an effort to introduce more inclusive language to technology?

A. That is correct.

Q. So rather than using white hat hacker, can you describe that term and what the current terminology is?

A. Yeah. There's a number of terms floating around. We call it good-faith security researcher, or the other term that comes around is ethical hacker. It's basically a hacker who's, once again, hacking for good. Their ultimate goal and objective is to make organizations and the industry safer.

Q. What is the now accepted term for what used to be referred to as black hat hacking?

A. We usually call them malicious attackers or malicious hackers.

Q. What are some of the foundational principles that separate good-faith security research or ethnical hacking from malicious hacking?

A. It ultimately goes to what your objective is, right. If your objective -- like if I'm finding security vulnerabilities and I'm coordinating with companies to get those vulnerabilities remediated, or coordinating with the industry as a whole to get those remediated, I am doing good-faith security research. If I'm attacking organizations for the sole purpose of, say, financial gain, or I'm attacking organizations for the sole purpose of prestige in the community, and my goal is not improving the industry as a whole, then I would not be doing good-faith security research.

Q. Is financial gain the only kind of personal gain for malicious hacking activity?

A. Absolutely not. Absolutely not. There's a ton of people in the security industry that do security research for something that is not financial. For example, you would -- let's say a malicious attacker would break into some place and then they would be able to brag about it on Twitter or someplace else, that's, you know, building up your prestige in the community. We do see people that do that type of attacking.

And also, I got to thinking about it, there's a number of security researchers that do academic work that they're probably not making very much money because they're professors, but they are absolutely contributing to the state of computer security, not necessarily from the financial aspects of it.

Q. Okay. Is there a difference between secure -- or research, in the broadest sense, and good-faith security research?

A. Yeah. There are some people in the industry, although it's fewer now than it was 15, 16 years ago, that they're doing security research for the purpose of research and their own edification.

An example would be if we went back a long time ago, there were people that were doing security research. And if we go back 15, 16, 17, even 20 years ago, if you found a vulnerability and you went to a company, the first thing that company tried to do was to threaten you with a lawsuit, threaten you with legal action, or try to get you to sign a nondisclosure agreement. And that was years ago.

And computer security is still really, really new as a field, but over time, we have seen more and more organizations embrace bug bounty programs, responsible disclosure programs, where they work with security researchers to fix those vulnerabilities. So we now see fewer and fewer security researchers that are just doing it on their own completely on the underground, not really trying to break into anything to steal anything, but just seeing what they can actually do. We're seeing that becoming rarer and rarer because the industry is so open to a number of different programs that exist for a security researcher to not only not get in trouble, but actively get paid and recognized in the industry as well.

Q. Are there norms of -- or standards of conduct that are generally accepted in the information security community?

A. Yeah. So are you talking specifically in vulnerability research?

Q. Yes.

A. One of the things is do no damage, right. So if you're doing vulnerability research, a lot of times it's very easy to download software. For example, Microsoft Office; I can download Microsoft Office and I can do security testing at home and that doesn't impact anybody. If I start doing vulnerability research against a live company, let's say they have a bug bounty program and that's somewhat authorized for me to do, I wouldn't do denial of service tests. In fact, in many of the organizations that are out there that support vulnerability research, like Bugcrowd, and HackerOne, in their standards they say you're not allowed to do destructive testing against an organization. They also put limitations on what you're allowed to download.

Many organizations, like EC-Council and Bugcrowd and I think HackerOne, they say if you're doing security research, you're absolutely supposed to limit the amount of data that you gain access to.

An example would be, I can access a database. Think of a database as a spreadsheet with lots and lots and lots of rows. I can download that entire database to prove that there's a vulnerability, or I could do a query to see how many records exist on that database. Both would prove that there's a vulnerability, but only one of those would lead to data leaking onto my computer.

Q. Are there circumstances -- so is it typical in your company to do a pen test with permission?

A. Always.

Q. Okay. What does that permission structure look like?

A. So the permission structure for Black Hills Information Security is a company will contact us. They will request a security assessment. We will talk with them what their goals and objectives are, anywhere from breaking into their company to doing vulnerability research on a product that they want us to do an assessment on. Then we set up legal frameworks where there's memos of understanding, and we set up a rules of engagement on how we're supposed to test, when we're supposed to test. We clearly identify the scope of what we are to test. And then after upon -- all the agreed-upon times, we actually start testing them, but only after lots of communication on what exactly we're supposed to test and how we're supposed to test.

Q. Even in those situations where a company has hired you under contract, under all those, you know, parameters to test their systems, will you delete logs as part of your pen test?

A. Never once.

Q. Why not?

A. Because if you look at a log, a log is a running record. Think of like a financial accounting record. If I was running a business and I didn't keep a general ledger, accounts payable, accounts receivable, my business may still function, but I wouldn't have any visibility into the finances.

When you think of a computer, a computer is generating logs explaining what it did. And if something goes wrong, those logs are used to troubleshoot and figure out exactly what happened. So by us doing security assessments, if we delete logs, we may be deleting something that could be used for financial processing.

For example, big cloud providers, companies will track their logs to see utilization and help track how much CPU, bandwidth, data transfer they're doing, because that directly impacts their cost.

Also with logs, logs will be used in forensics engagements.

So let's assume that there is an organization that is compromised, those logs are used for us to reverse what the attackers did. If you get into a situation where I am hired and I delete those logs from a company, then that really calls into question their entire logging infrastructure. And I may get into trouble saying that there's an active attack, that I just deleted some evidence associated with that particular attack.

So logs are absolutely essential for computing today.

Q. In a situation where you're under contract and you have permission to do a pen test, would you ever create key pairs and security groups on your customers?

A. No, we wouldn't do that. And the reason why is any time we get -- well, we wouldn't do that unless we got explicit permission from the customer to do that. The reason why is whenever we start changing the security configuration of an organization, there's a very real possibility that we may impact operations. So if you start messing with security groups, you start messing with key pairs, you start opening ports and firewalls, you may be opening up that customer to follow-on attacks or another attacker coming in. You may introduce something like a rule that is -- then supersedes another rule or creates a conflict in the security rules.

And in some tools, they have this tool called "fail secure," for some tools, where if there's a conflict it just shuts down, and we may impact operations.

So we would never do something where we would actively change the security state of a customer unless we had explicit permission from the customer where we tell them, this is what we would like to do, this is why we would like to do it, and here are some potential consequences of us doing that.

Q. I'm sure there are situations both in your business or maybe even recreationally where you run across a vulnerability that you didn't anticipate?

A. Yeah. That -- that actually happens quite often where we're testing a company and we may find a vulnerability in a piece of software that that company uses.

We had one customer we were testing and we found a vulnerability in their two-factor authentication systems, you know, like your phone or a key fob or something like that. And it was actually a vulnerability in the two-factor vendor that our customer was using. That requires us to do disclosure with our customer and working with our customer to coordinate a disclosure with the vendor as well.

Q. And so you mentioned that there is a disclosure process. Is that, again, based on the norms and standards of the industry?

A. So there -- when we're looking at norms and standards of the industry, if you look at the majority of like Fortune 500 companies, they are working now to set up vulnerability disclosure programs. And they have to do this for a couple of reasons. One is their customers may identify vulnerabilities in the day-to-day usage of an application.

So if anyone has ever used an application and it crashes, that is something that a lot of attackers like to take advantage of, because we can many times leverage that crash and turn it into an exploit. So they need to have those programs where their customers can let them know that there's something wrong with their software.

In addition to that, with the open community, good-faith security researchers, many organizations have programs where you can send an email to that company's security team and then start the process of working with that company to remediate those vulnerabilities.

Q. Is there a general consensus within the information security community about some of the conduct that crosses a line into malicious hacking?

A. Yeah. Anything that could potentially cause damage or lead to a leak of data that is not yours. Those are kind of the two main areas that we generally stay away from, even if you're doing a bug bounty, even if you're doing a penetration test, once again, anything that can cause a crash to a computer system.

Or another example would be if I don't have permission from a customer, I would never upload malware to a computer unless I had explicit permission to do that. And I wouldn't download a tremendous amount of data from my customers, either.

So a couple of examples: If I'm pen testing a hospital, if I download all of the medical records for that hospital, then my company has to adhere to HIPAA, which is the Healthcare Information Portability and Accountability Act, and that has a lot of security controls that I would then be beholden to.

If I attack a bank or a credit card processor, if I download a bunch of credit card information, there's a group called PCI, Payment Card Industry, that sets up security standards for processing and storing credit card information. My company would have to be beholden to those security standards as well.

So, generally, we try not to download any more data than is absolutely necessary for us to prove that a vulnerability exists.

Q. What about cryptocurrency mining, using other people's resources, is that considered to be a good-faith security practice?

A. Yeah, we would never do that.

And there's -- once again, there's a number of reasons for that.

THE COURT: Wait, wait. She didn't ask you that yet, so --

THE WITNESS: Oh.

THE COURT: -- he would never do that.

Q. (By Ms. Manca) Are there reasons that you would not install cryptocurrency mining on other people's computers?

A. Absolutely. Two main reasons: One, none of our customers would ever give us permission to do that. And the reason why they wouldn't give us permission is cryptomining, depending on the currency, generally tends to be CPU and GPU intensive, and that may impact computer systems and operations.

So if you think of cryptomining, it's doing a mathematical function over and over and over again, at very high rates of speed, and that could definitely cause an impact to operations.

Q. What about exploiting a vulnerability on one date, not saying anything to a customer, and then coming back to exploit the same vulnerability, would that be consistent with good-faith security research?

A. So if we go back to the old "hats" terminology, we used to have white hat, which is people that were doing good-faith security research, we had black hats that were breaking into computer systems, and then there used to be a term called "grey hat hacking." And that would fall in that legacy term of "grey hat hacking" where people were hacking not causing any damage, identifying vulnerabilities, but they were doing it for just themselves they weren't sharing it with the community, they weren't trying to break into steal anything, they were just basically proving they could gain access and nothing more.

Q. Does that qualify as good-faith security research under current norms?

A. No, it wouldn't qualify. In fact, most organizations would -- they go out of their way to say, don't gain access and, specifically, don't violate any laws.

Q. You mentioned that, you know, you advocate for being able to test companies to expose vulnerabilities; is that fair to say?

A. That is a fair assessment.

Q. Do you also believe it's important to have clearly defined standards governing offensive hacking?

A. Absolutely. It's absolutely essential for us to develop standards as far as where the lines are, because, once again, if we go back 15, 17, 20 years ago, there were no standards, so you had this problem in the industry where any hacking that you did or any security research that you did could get you into trouble.

As we've developed these standards, we've created outlets for security professionals to do security research, do it in a safe way, coordinating and working with companies, and working with companies that will reward you for doing that security research. And we've had to do that as a protection mechanism so that -- this is a new industry, we want to do it legitimately, because trying to protect IT everywhere is something we should all be interested in.

MS. MANCA: I don't have any further questions. Thank you, Your Honor.

THE COURT: Mr. Klein?

MR. KLEIN: Yes, I do have some questions, Your Honor.

THE COURT: Sure.

CROSS-EXAMINATION

BY MR. KLEIN:

Q. Good morning, Mr. Strand.

A. Morning.

Q. I'm Brian Klein. I represent Paige Thompson.

A. Good to meet you.

Q. We both need some water.

Even today, some people in your industry are still afraid to report vulnerabilities, aren't they?

A. Could you repeat that?

Q. Today, some people in your field are still afraid to report vulnerabilities to companies, aren't they?

A. Absolutely.

Q. And that's because companies sometimes don't fix the problems.

Is that a "yes"?

A. That is correct.

Q. Companies sometimes threaten to sue the person?

A. That is also correct.

Q. Including under the Computer Fraud and Abuse Act?

A. That is absolutely correct.

Q. And sometimes companies even report those people to law enforcement?

A. That is also absolutely correct.

Q. You talked about how the norms of the industry have been evolving over time, right, and that -- what was it like 10, 15 years ago, it was a little bit more -- it was the real wild west maybe?

A. I don't -- didn't use the term "wild west."

Q. I'm using it.

So there was not a lot of guidance, not a lot of rules, 10, 20 years ago?

A. That is absolutely correct.

Q. And as you sit here today in 2022, June, the rules still aren't settled; right?

A. No.

Q. They're still evolving?

A. No. And that's true for any industry, rules are constantly evolving.

Q. And these aren't laws, these are just norms in the industry; right?

A. That is correct.

Q. So good-faith researcher, that's just something, as you sit here today, that's where the industry's head might be, but it could change two, three years from now?

A. That is correct.

Q. And two or three years ago, it might have been different?

A. It was different.

Q. You mentioned that -- you work for a pretty large firm. How big is your company?

A. About a hundred employees.

Q. Okay. And you have lawyers on staff?

A. No. We do not have lawyers on staff.

Q. You use outside law firms?

A. We do use outside law firms specifically for looking at our contracts when needed.

Q. Okay. And you have a big network of support when you run across an issue or to find issues, computer vulnerabilities?

A. In what context, within the company or the outside?

Q. Yeah. It's not just you on your own doing this, you're working with a team?

A. When I started, it was just myself. In 2008, before that, before I started Black Hills Information Security, there was a good seven years where I was by myself.

Q. So a lot of people do do this by themselves then; right?

A. Yes. There are hobby -- especially with bug bounty programs that exist today make it so much easier to do this with some support.

Q. So there's people who are amateurs who don't work for a company and do this type of computer research?

A. I wouldn't call them amateurs.

Q. What would you call them?

A. They're still highly technical. They're very, very professional. When you're looking at some of the people that do vulnerability research, they're very, very skilled, even though it may not be their day job.

Q. And there may be people who are grad students who do this?

A. Absolutely. All academic levels, and people without degrees as well.

Q. People without degrees, people who are unemployed?

A. Absolutely. In fact, we've hired some of those people as well.

Q. Okay. I want to circle back again to the concept of responsible disclosure.

A. Uh-huh.

Q. That's a concept that's been evolving over time; right?

A. It has, absolutely.

Q. And some companies use -- as we sit here today, use websites like HackerOne?

A. Uh-huh.

Q. Some companies have their own internal programs?

A. Uh-huh.

Q. Some companies have no program?

A. That is also true.

Q. And sometimes it's confusing to find out how to report a vulnerability, isn't it?

A. I would say it's always confusing to find out where to report a vulnerability, but with -- I would say -- let's -- for most organizations, 10 minutes on Google, you can figure it out.

Q. But it's confusing sometimes, right? Or always confusing, frankly, is what you just said?

A. Yeah. But like I said, a little bit of research, probably you can find out from most organizations in less -- I would say, 10 minutes to half an hour, pretty easily, to find out who the security team is there.

MR. KLEIN: One second.

THE COURT: Sure.

(Off the record.)

MR. KLEIN: Nothing further, Your Honor.

THE COURT: Okay. Thanks, Mr. Klein.

MS. MANCA: Very briefly, Your Honor.

THE COURT: Just briefly, Ms. Manca?

MS. MANCA: Maybe lengthy. No, not lengthy. Thank you.

REDIRECT EXAMINATION

BY MS. MANCA:

Q. Mr. Strand, even when rules are evolving, is there still conduct that over time, even looking back 15, 20 years, was clearly past those lines?

A. Absolutely. Specifically in the area of creating damage, that has always been across the line. Doing something where you're running your own software unauthorized, like a malware, like back door or virus, that has always been crossing the line. And I would say downloading data that is not yours has always been crossing the line in the industry.

Q. And was the guiding principle of good faith always the same?

A. I would say as it's evolved over time, right, like the terminology grey hat, white hat, black hat, moving to ethical hacker, malicious cracker, we had all these terms over time. But, yes, within that terminology of, you know, good faith being white hat, absolutely, evolving into ethical hacker or good-faith security researcher, those principles have stayed true.

MS. MANCA: Thank you. No further questions.

THE COURT: Anything else, Mr. Klein?

MR. KLEIN: No, Your Honor.

THE COURT: Okay. So this is opinion testimony, which I've allowed here today, but I do want to emphasize, there's a difference between the standards in the industry and the crimes charged here, so just to be clear about that.

Thank you very much, Mr. Strand. You may step down.

THE WITNESS: Thank you, sir.

THE COURT: Okay. Let's take the midmorning break now.

And I need to talk about a few things with the lawyers, so this one will be more like 20 to 30 minutes.

So, Victoria, you can take them next door, but probably won't come for you quite as quickly as the usual morning break, all right?

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Thank you. Please be seated.

So is the government pretty much ready to rest its case? Didn't want to push you with the jury here.

MR. FRIEDMAN: We are, Your Honor.

THE COURT: Okay. So when the jury comes back, I'll have you rest your case.

And I think all the exhibits have been ruled on that were dangling.

So would the -- you have a number of remote or virtual witnesses. What's -- are these all Capital One or AWS witnesses or?

MR. HAMOUDI: They are Capital One, AWS, and Michigan State, and Ohio. And we provided a witness list to the government last night.

We have a -- one witness, Mr. Carstens, we filed a memo on, and I anticipate the government is going to be objecting to his testimony.

And we -- I know the Court wants to move the case along, but with respect to deciding -- giving Ms. Thompson advice on the Fifth Amendment, and Mr. Halderman, we would like to have the night, Your Honor, and put that testimony on tomorrow if the Court will grant us that leave, because we may run out of time is basically what I'm telling the Court.

THE COURT: Yeah, it's okay. And I'm fine with you taking some time to talk to Ms. Thompson about whether she wants to testify or not.

And then Professor Halderman is your expert witness?

MR. HAMOUDI: Yes, yes.

THE COURT: And you'll make a decision about whether you call him also overnight?

MR. HAMOUDI: Yes, Your Honor. Yes.

THE COURT: Okay. And then in terms of the virtual witnesses here, Mr. Edgar, Mr. Ortiz, Mr. Schmidt, Mr. Hopkins, Mr. Nolan, and Ms. Lye, how long do you anticipate their testimony?

MR. HAMOUDI: I don't anticipate it to be very long. We intend to put 'em on, ask very targeted questions, and get 'em moving along, Your Honor.

THE COURT: All right. So you may actually have more like a half day of testimony.

MR. HAMOUDI: Yes.

(Off the record.)

MR. HAMOUDI: Oh, a couple of things, Your Honor. We -- there was the matter of the contract issue.

THE COURT: Right.

MR. HAMOUDI: And I -- I think Mr. Newby's here, got stipulation language from Mr. Newby, I've offered it to the government, I'm waiting to hear back from them on that issue. So that could resolve an issue there.

And then we needed to elicit a single question from Mr. Brandwine, who testified yesterday that we forgot to ask. We're trying to reach a stipulation with the government as to that fact. He's also teed up virtually, but we're trying to resolve that with the government as well.

THE COURT: Okay. In regards to those last matters, Mr. Friedman, the sample or model contract with AWS and Mr. Brandwine, are you ready to talk about those or?

MR. FRIEDMAN: Partly, Your Honor.

THE COURT: Okay.

MR. FRIEDMAN: With respect to Mr. Brandwine, we had proposed a slightly edited version that we would agree to. I don't know whether that's going to satisfy or not.

THE COURT: Okay.

MR. FRIEDMAN: And with the other, we just received that request this morning, so we need to look at that and are not really ready to talk about that.

THE COURT: And you are objecting to Mr. Carstens' character evidence?

MR. FRIEDMAN: We are, but I would defer to Ms. Manca to make that argument.

THE COURT: Sure. Yeah. Okay.

MS. MANCA: Are you like ready to hear that? Sorry. Thank you.

Your Honor, this witness was not on the defense witness list. I know that notice is not particularly an issue that the Court may care about, but we are troubled by the fact that this witness was likely known to the defense as early as 2019 because he presented in the context of a detention argument in 2019 and was endorsed last night.

But with respect to the admissibility of his testimony, character evidence requires evidence of reputation in the community, and the community has to be broad enough such that it's an accurate representation of what people within that community would think.

The defense has not provided any information about what the particular community would be that Mr. Carstens would be testifying about. And without knowing that information, there's really no basis to judge whether that community is valid for purposes of offering reputation or opinion testimony.

So that's the basis of our objection.

THE COURT: I've never heard of such character evidence before in this way, so I need to take a look at it. And I did kind of breeze through the memo, but I haven't looked at any cases, so give me a little time to do that.

MR. HAMOUDI: Thank you, Your Honor.

THE COURT: And -- yeah.

MR. HAMOUDI: Just to give a little preview, I've never really understood how these statements, all of these statements, were going to play out in this case. And there's volumes, volumes of these tweets and Internet Relay Chats. And there's been really no circumstance provided to the jury, right. Like the other party talking, right. So they're just sort of these statements sort of out there.

And where Mr. Carstens' testimony is really targeted towards is to -- is really for non-hearsay purposes, that -- to provide some context to the jury. And I certainly think that that issue has clearly been opened. And that's been a challenge in this case because -- because -- because I think that, you know, there's clear evidence that Ms. Thompson was internally struggling. And I speak to that -- I'm trying to speak to that in a very dignified way. And I think it would be an injustice for this jury not to hear from somebody like Mr. Carstens.

So that's my position. Thank you for looking into that.

THE COURT: Sure. Okay.

So let's do this. Victoria, do we have the remote witnesses all set up like we did yesterday or do we need some time for that?

THE CLERK: I just need about five minutes.

THE COURT: That's all?

(Off the record.)

THE COURT: Why don't we do this, let's do -- let's bring the jury back about 10 of 11:00, we'll do -- the government will rest its case, the defense will do a couple of virtual witnesses, and depending on how far we get, maybe I'll send the jury home at noon and we'll use this afternoon to go over the legal issue, finalize the issue of the AWS contracts, and finish up the testimony tomorrow, and maybe either do instructions and closings Wednesday, or maybe just do them Thursday, give you a little time to get organized, and maybe even finish up the remote witnesses today and then do -- you have some time to think about the Professor Halderman and whether Ms. Thompson will testify, kind of play it by ear there. But I'll give you tonight to do that for sure.

MR. HAMOUDI: Thank you, Your Honor.

I would just -- the Rule 29 also at some point would be handled today, is the Court...

THE COURT: What's Rule 29?

MR. HAMOUDI: Once the government rests, we would file for --

THE COURT: Oh, your motions on the -- the legal motions, yeah.

MR. HAMOUDI: Yeah, just orally -- orally -- I orally have to make a record.

THE COURT: Yeah. Thank you for not calling them halftime motions. That's one of my pet peeves.

Sure, after they -- after they rest -- well, why don't we do this, Mr. Friedman, go ahead and rest your case, then you can note your motions to dismiss at the end of the government's case and just sort of summarize them, and then we'll take our break.

Is the government ready to rest its case?

MR. FRIEDMAN: We are, Your Honor.

THE COURT: All right. The government has rested its case.

Mr. Hamoudi, you want to make your motions under Rule 29?

MR. HAMOUDI: Yes, I do, Your Honor.

Your Honor, just based on the evidence that the government has presented, I do want -- I want to raise two Constitutional objections. One's fair notice and the second is the First Amendment.

And in recent years, the Supreme Court has confronted attempts by the government to shoehorn misconduct into ill-fitting federal criminal statutes. The Supreme Court has repeatedly rejected government's attempts to expansively read criminal statute, to creatively reach conduct the government characterizes as bad faith.

And, for example, one of those cases is *Bond v. United States*, and that's at 572 U.S. 844. And that case, the Chemical Weapons Convention Implementation Act was used to reach a wife who attempted to injure her husband's lover by spreading chemicals on a car door, a mailbox, and a doorknob.

And more recently, the government attempted to creatively apply the same wire fraud statute here in *Kelly v. United States*, and that's 140 S.Ct. 1565. And in *Kelly*, public officials changed the direction of traffic entering New York City as political retribution, the so-called Bridgegate scandal. And the Supreme Court there reasoned that the loss to the victim of any services was only incidental, and the time and labor from the employees rerouting the traffic were just the implementation costs of this scheme, not the object. And the court cautioned there, Your Honor, it cautioned allowing the federal government to use the wire fraud statute to accomplish a sweeping expansion of federal criminal jurisdiction.

And part of the problem, Your Honor, with creative and novel application of federal criminal liability is that it runs afoul of the fair notice that due process requires. A statute must give ordinary people notice to say that they can understand clearly what conduct is prohibited and prevent arbitrary and discriminatory enforcement. If not, the statute is void for vagueness as applied, not -- not facially, but as applied.

And as applied to the facts here, Your Honor, the government's theory undermines fair notice. Nobody anywhere, anywhere in the country has been prosecuted for wire fraud for doing what Ms. Thompson has done in this case, which was nothing more than research, downloading, computers that allowed access to their resources and data. Her acts are indistinguishable from what academics and researchers do every day right now. And -- and so that is the conduct at issue.

And the other thing is this, Your Honor, unlike the highly regulated commodities markets, the stock market, the SEC, all of these you have to have licenses, you go through -- the government has incredible oversight over these industries. This is not an industry that is regulated. It is like the wild west. These strange rules about registering with HackerOne and how you approach people. Companies are paying people money, they pay money for them to show that the customer's information is not safe or it's been downloaded, and they enter into nondisclosure agreements.

You know, researchers come in all shapes and sizes and they come from all stations in life. And this is the first case, again, where these laws are being applied in a manner that they are, and that in and of itself, we contend, is a notice violation. There was no case in 2019, a published case that said, you do this, you violate the CFA Act and you violate the wire fraud.

Now, I want the Court -- I want to make arguments on the access device fraud and aggravated identity theft because I think there is literally no -- those counts should not be going to the jury, Your Honor. The government's evidence failed to show that Ms. Thompson knowingly and with the intent to defraud possessed 15 or more unauthorized access devices.

And to be convicted for access device fraud, Ms. Thompson must have known the devices were unauthorized, acted with the intent to deceive and cheat, and affected interstate commerce. The data was not usable.

Access device refers to a means of account access that can be used to obtain money, goods, services, or anything of value. And that's 18 U.S.C. 1029(e)(1). The phrase can be used requires that Ms. Thompson's information must be usable, capable of obtaining value. And that's *United States v. Onyesoh*, 674 F.3d 1157.

The government's evidence of usability was limited to Internet searches related to credit cards over the course of 30 minutes, well prior to her arrest. That's Government's Exhibit 504.

In addition, Ms. Thompson appears to have created a list of information for one Seattle residence, that was Mr. Baleda, whose favorite food appears to be pizza, and that's Exhibit 782.

No evidence was presented that Ms. Thompson ever took any steps to actually sell the data or create fake credit cards.

The second element that no rational jury could find on is unauthorized. The possession of access devices is unauthorized when the devices are stolen or obtained with the intent to defraud, and that's 1029(e)(3). Intent to defraud requires an intent to deceive and cheat, to deprive the victim of money or property by means of deception. Based on the evidence presented at this trial, no rational juror could find that Ms. Thompson ever stole the information or presented it with that intent. The server automatically granted Ms. Thompson access to information after she entered commands that Amazon -- that Capital One made available. And this hardly constitutes stealing.

So no rational juror, Your Honor, could find that Ms. Thompson was stealing, was lying, let alone have any intent to do so.

There's also no evidence that Ms. Thompson intended to deprive someone of property through fraud. The government relies on Ms. Thompson's computer search history, files, and empty threats to disseminate the information.

To reiterate, the government points only to these Internet searches that were never followed up on and took places within that 30-minute time span before Ms. Thompson's arrest.

The only evidence resembling follow-through for Ms. Thompson's threat is that she supposedly grouped information of Seattle residents in a manner consistent with intending to use the information for fraudulent purposes. This is Docket 255 at 18. This is what they are saying. This is their position that they have taken. These actions, Your Honor, do not establish an intent to cheat because Ms. Thompson never verified the personal information, acquired an embosser, visited a carding forum, contacted a scammer, or even searched for a credit card application.

And there was certainly no attempt to commit access device fraud, Your Honor. The government -- to convict Ms. Thompson, the actions must cross the line between preparation and attempt by unequivocally demonstrating that the crime would take place unless interrupted by independent circumstances. This is *United States v. Goetzke*, 494 F.3d 1231. Any rational juror will find that the government fails drastically short of this standard. Even if Ms. Thompson had everything she needed to defraud Mr. Baleda, which she did not, the statute requires an attempt to possess not one, but 15 unauthorized devices. Nothing unequivocally demonstrates that but for her arrest, fraud would have taken place. No rational juror, Your Honor, could find an attempt to violate that statute.

THE COURT: Mr. Hamoudi, I don't want to interrupt you, but I think Ms. Thompson could use a little break.

MR. HAMOUDI: Yes.

THE COURT: So why don't we take a little break. I'll take this under advisement. You can finish the argument.

MR. HAMOUDI: Just for the record, we have to say, we raise it as to all counts.

THE COURT: To all counts, yes.

MR. HAMOUDI: Yes.

THE COURT: Okay. Thank you.

All right. Let's do 11:00.

And we'll -- I'll have the government get up and rest its case in front of the jury, and then we'll do one of the virtuals, okay?

And if you need more time with Ms. Thompson than 11:00, just let Victoria know, all right?

MR. HAMOUDI: Thank you, Your Honor. We really appreciate it.

THE COURT: Okay. Absolutely.

We'll be adjourned.

(Court in recess 10:42 a.m. to 11:09 a.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Are we ready for the jury?

MR. KLEIN: One of our first witnesses, Steve Schmidt, and we're going to ask a very targeted question about his conclusion that this attack was not an SSRF attack.

THE COURT: As done in the letter.

MR. KLEIN: Very focused on the letter, and that one part of it, the conclusion.

I talked to the prosecutor about this, and he indicated he thinks that opens the door to a lot of other questions and areas. And we're trying to keep the scope very limited, and I don't think he should be able to exceed the scope, or that conclusion, but I'm worried that we're going to have a lot of questions that require a lot of objections.

MR. FRIEDMAN: You know, obviously, we would stay within the scope of that. But if the question is, "Do you believe this is an SSRF," it is not possible to cross-examine him on that without saying what happened here, what's an SSRF, and how do they compare. I mean, I'd have to ask those.

THE COURT: Mr. Friedman has got to stay within the purview of the topic, but within the purview of the topic, he's not limited to just the conclusion.

MR. KLEIN: Yes, Your Honor.

THE COURT: Okay. Great.

All right. Victoria, you can bring the jury in while I talk to the lawyers.

MS. MANCA: And this was an exhibit issue. Ms. Erickson said 715 was displayed to the jury twice. It should be admitted for illustrative purposes only. I don't believe the court made a ruling on that, but we'd offer that for illustrative purposes, given that it's been displayed to the jury.

THE COURT: Okay. 715 is admitted for illustrative purposes only.

(Government Exhibit 715 admitted.)

MR. KLEIN: Your Honor, we might call Mr. Schmidt after lunch. I want to think about Your Honor's...

THE COURT: All right.

The first one will be?

MR. KLEIN: Mr. Brandwine.

THE COURT: Okay. Let Victoria know when she comes back.

MR. KLEIN: I will.

THE COURT: Are all the Capital One witnesses going to be testifying from the same place, or different places?

MR. KLEIN: I think they're all in different places, Your Honor, their homes or their offices. When we tested this morning, they looked to be in different places.

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY

THE COURT: Thank you. Please be seated.

All right. Welcome back.

Mr. Friedman?

MR. FRIEDMAN: Your Honor, at this point, the government rests.

THE COURT: Okay. The government has rested its case, and we'll move to the defense, which will call -- they have no obligation to call witnesses, but they are going to call some witnesses. And the first one, Mr. Klein?

MR. KLEIN: We are recalling Eric Brandwine, Your Honor.

THE COURT: All right. Mr. Brandwine testified yesterday, but they're recalling him. All the witnesses need to make themselves available, and Mr. Brandwine is going to appear, hopefully.

THE CLERK: I've just admitted him into the Zoom.

THE COURT: Mr. Brandwine, you're still under oath, and we just have very few questions for you from Mr. Klein. Okay?

THE WITNESS: Okay.

ERIC BRANDWINE,
having been previously sworn, testified as follows:

DIRECT EXAMINATION

BY MR. KLEIN:

Q. Mr. Brandwine, can you hear me?

A. Yes.

Q. Good afternoon, because I believe you're back East.

A. (Nods.)

Q. When were you first interviewed by the FBI and prosecutors in this case?

A. I believe it was mid to late April, perhaps, April 21st of this year, 2022.

MR. KLEIN: Thank you, Mr. Brandwine. Nothing further.

THE COURT: Ms. Manca?

CROSS-EXAMINATION

BY MS. MANCA:

Q. Hello, again, Mr. Brandwine.

You don't know when the government received information about your identity, do you?

A. No, I have no information about that.

Q. So for all you know, it was the week before the interview?

THE COURT: The questions are not evidence, and he said he didn't know.

Thank you, Mr. Brandwine. I appreciate you making yourself available to us.

THE WITNESS: All right. Thanks.

THE COURT: Next witness?

MR. HAMOUDI: Diane Lye, Your Honor.

THE CLERK: I'm admitting her now.

THE COURT: Okay. So can you hear us okay?

THE WITNESS: Yes, thank you.

THE COURT: I'm Judge Lasnik here in Seattle, and my clerk is going to swear you in, so could you please stand and raise your right hand?

DIANE LYE,
having been first duly sworn, testified via Zoom as follows:

THE COURT: Thank you very much. Please be seated.

THE CLERK: Please state your first and last names, and spell your last name for the record.

THE WITNESS: Diane Lye, L-y-e.

THE COURT: All right. Thank you, Ms. Lye.

Mr. Hamoudi, Paige Thompson's lawyer, will ask you some questions now.

DIRECT EXAMINATION

BY MR. HAMOUDI:

Q. Good morning, Ms. Lye. How are you?

A. I'm fine. Thank you.

Q. Where do you work?

A. At Capital One.

Q. And where did you work in 2019?

A. At Capital One.

Q. And what was your position at Capital One?

A. At the beginning of 2019, so from January until November, I was the senior vice president of technology for Mosaic Technology, which was the enterprise data technology organization.

In addition, from March -- from May, May the 1st of 2019 until the present, I was the executive vice president and divisional CIO for card technology.

Q. And are you familiar with the data-breach incident involving Capital One's data?

A. Yes.

Q. And were you tasked with analyzing the data obtained in that breach?

A. I was tasked with the technology support that enabled the analysis of the data in the breach.

Q. And do you recall how much data was involved in the breach?

A. In total, there were just under 100 million consumer identities that were involved in the breach, with the most significant piece of the data involved in the breach being around 120,000 Social Security numbers.

Q. And from a data perspective, not the identities, does 1.7 terabytes sound right about the total amount of data that was downloaded from Capital One?

A. Yes.

Q. Okay. And I want to ask you some questions about a team and yourself that undertook a process with the data. Do you recall doing that?

A. Yes.

Q. And what did you undertake, that team and yourself?

A. Yes.

Capital One, obviously, had an obligation to inform consumers whose data had been taken during the breach. And that obligation did not extend to all the 98 million, nearly 100 million; it extended to those customers who had the most sensitive data; the Social Security number or the bank account number had been taken.

And I led the team that went through all of the S3 buckets and the 2.4 million objects in those S3 buckets from which data had been taken in order to piece together the data that we could use to, first of all, identify how many consumers were impacted, exactly which fields had been taken, and which consumers we needed to notify.

Q. And you talked about the buckets. As you recall, if you do, there was a total of 190 buckets that were downloaded, correct?

A. Yes.

Q. And of those 190, 31 of those contained customer data, correct?

A. Thirty-one of those, yes, contained consumer data, yes.

Q. And so the process that you went through was to go through 2.6 (sic) million objects, correct?

A. Yes.

Q. And an object is a file, correct?

A. Yes.

Q. And identify which of those files contain customer data?

A. Correct.

Q. And you were only able to do that because you had deep-subject-matter experts in the software applications that owned those buckets, correct?

A. To assemble the data back together, we needed that subject-matter expertise in the data. Unfortunately, however, there was at least one file that contained data that didn't need assembling back together, where there was Social Security numbers immediately next to other identifying data.

Q. You previously testified in a deposition, do you recall?

A. I do.

Q. Yeah. Do you remember saying that the process was a bit like putting together a jigsaw puzzle that has 2.6 million pieces and you don't know the picture?

A. That is exactly what I said.

Q. And you said that -- you also said that that's kind of the way to think of this process, if you don't know the process, to understand how that matching and assembling would take place, correct?

A. Correct.

Q. And, in fact, you had to use data that was not even part of the breach in order to understand the identities of the customers who owned some of these accounts, correct?

A. Correct.

Q. And you opined, as a subject-matter expert, during that testimony that it would have been absolutely impossible for Ms. Thompson to go through that process, correct?

A. That's correct. But at the time of that deposition, I was not aware of the two log files where there were customer Social Security numbers in clear text that were immediately next to other identifying information.

So for the overwhelming majority of the data, we needed to put the jigsaw puzzle pieces together. However, there was a smaller piece of the data, a smaller fraction, that we discovered later, where you didn't need to go through that jigsaw-puzzle assembly.

Q. And to follow up on that, were you ever provided any information that Ms. Thompson ever saw that data, which you discovered later?

A. I don't know if I'm allowed to answer that because it was discussed in my preparation yesterday.

Q. How long did it take you to become aware that, out of all of that data you had reviewed through these processes, that there was a small fraction of data that was left out?

A. I learned about the small fraction of data that was left out late in January of 2021, when we were asked to, essentially, redo the whole analysis because of a concern that we might have left some data out.

Q. And then -- so when you testified about that first time you went through the process, that was in June of 2020, correct?

A. The first time we went through the process of assembling the jigsaw puzzle, that was actually in July -- that was in July of 2019, and then my first deposition was in June of 2020.

Q. Okay.

MR. HAMOUDI: All right. Ms. Lye, really appreciate you taking the time to testify today.

The prosecutor may have some questions.

Thank you.

THE COURT: All right. Mr. Friedman, the Assistant United States Attorney, will ask you some questions now.

CROSS-EXAMINATION

BY MR. FRIEDMAN:

Q. Good morning, Ms. Lye. How are you?

A. I'm fine. Thank you.

Q. Okay.

You were asked some questions a moment ago about things you had said about whether Ms. Thompson could review or access data; do you recall that?

A. I do.

Q. And you talked about the greater mass of the data when you were talking about that, correct?

A. Correct.

Q. Okay. Was much of the data that was taken in this case from something called the Capstone System?

A. Yes.

Q. What is the Capstone System?

A. The Capstone System is -- it was the system that we used for deciding whether or not an applicant, somebody who applied for a credit card, would, in fact, be given a credit card.

So it was the customer-acquisition system that included the decision about whether to give somebody a card and how much credit to give them.

Now, Capstone was a very old system, and by the end of 2018, we had begun retiring the Capstone System --

Q. Can I stop --

A. Sorry.

Q. Can I stop you there and ask a follow-up question?

A. Yes.

Q. Is that the data, or is that much of the data you were talking about when you were talking about whether it would be easy or hard to access that data?

A. Yes.

Q. Is that data in a particular format?

A. There was two chunks of Capstone data that were involved in the breach. There was a big analytic file that had 98 million customers in it that we were using because we were retiring Capstone, and that data was in a format called parquet, a data format for analysis that requires some expertise to access and understand and use; however, the metadata for that parquet was taken along with the data file. So that was one part of it.

The other part of the Capstone data were two log files, which were just raw dumps straight out of the system, that were discovered in January of 2021 and that we had missed in our original analysis.

Q. Okay. When you talk about the massive data here, was it data in the parquet format?

A. Yes.

Q. And is the parquet format a difficult format for people to work with? Is that what you're talking about?

A. Data in parquet -- parquet is a specialized format that supports analysis-use cases, data-science-use cases. So somebody with those skills could access that data set, but you would need to know -- have those skills.

Q. Was what Capital One was trying to do, though, much harder than what someone just trying to pull information out of there, perhaps for fraud, was trying to do?

MR. HAMOUDI: Objection.

THE COURT: Overruled. You can answer.

A. Yes. Because what we were trying to do is understand the full extent of the data that had been taken, generate a list of customers, find the contact information for those customers, and be able to tell those customers exactly what had been compromised.

So we were trying to put together the fulsome, complete picture; whereas, an individual with just that set of files could search within any file and find snippets of information about any particular person.

So they might not be able to complete the jigsaw puzzle, but they would certainly be able to see the color of the pieces, and that was something we were always worried about.

Q. (By Mr. Friedman) I'm going to show you an exhibit. It's page 2 of Exhibit 458, and it should show up on your screen.

A. Yes.

Q. So that's the first page, and here's the second page.

These are communications from someone paigeadele, or at least the top four, on something called Internet Relay Chat. On the second line, do you see paigeadele asking a question?

A. Yes, I do.

Q. And, obviously, it's going to be get very technical when we get to the file names, but what's the beginning of the question?

A. It looks like she's calling somebody called Jillian Lenox, "Have you heard of parquet?"

MR. HAMOUDI: I'm going to object. It's beyond the scope of my direct examination.

THE COURT: Overruled.

You can go ahead and answer the question.

A. Yes. It looks as though the question on the second line is directed towards someone called Jillian Lenox, and the question is, "Have you heard of parquet?"

Q. (By Mr. Friedman) And then is there a very long file path after that?

A. Yes.

Q. Okay. And what is the name of the file in that file path?

A. ASV, which our applications are often referred to as "ASV," so many of our file names at Capital One begin with the letters "ASV," "asvsbc" -- and "SBC" stand for "small business card" -- "linemanagement." So "line management" is the process of determining how large of a credit line a customer or an account had, and then "US-east-1" -- so "US-east" is referring to the AWS East region -- and then "/clip," and "clip" is Credit Limit

Increase Program, and then "gotoline-smallbusiness-internal," and then it looks like there's a date, which is 2019 February, and a time stamp, possibly.

So this is the identification and the location of our parquet file.

Q. Okay. So do you understand this to be Ms. Thompson asking or inquiring about a parquet file taken from Capital One?

A. Yes, I think that's what this is.

Q. Okay.

You also talked, on direct examination, about other data that was more easily accessible; do you recall that?

A. Yes.

Q. Okay. I think you said there were some log files that had Social Security numbers that were directly exposed or clearly readable?

A. Yes.

Q. Have you seen evidence that suggests that those files were files that Ms. Thompson looked at and recognized what was in them?

A. Yes, I have.

Q. Okay. I'm going to ask you to look at Exhibit 203, page 5, and if we can go down towards the bottom.

Do you see the tweet, just appearing on the screen, saying what Ms. Thompson has found in some of Capital One's data?

A. Yeah. It says "their," and I -- "their SSNS with full name and DOB."

Q. And have you looked at an actual file recovered from Ms. Thompson's computer and provided by the FBI to Capital One?

A. No.

Q. Okay. Let's take a look at Exhibit 713, page 1, and tell me if that is a file you looked at. We can blow up the text.

Do you recognize that as a file containing Capital One data?

A. It's a little hard to see.

Q. Would making it bigger help?

A. I don't think so, because I'm just seeing a bunch of headers. I'm not seeing anything that gives me -- oh, now, yes, I see, yes, "Capstone" is there.

Q. And if we could turn to page 5 of this exhibit, this appears to have some redacted information on the right?

A. Yes.

Q. Can you see what type of information in this filed contained in plain view?

A. These look like the -- yeah. So this looks like address with the state, the postal code, date of birth, Social Security number.

Q. Okay. And we've, obviously, redacted -- we've put the gray on there for purposes of this hearing, but the actual file contains unredacted Social Security numbers?

A. Yes, it does.

Q. Okay. And I want to show you one last file.

MR. FRIEDMAN: If we could turn to Exhibit 812, page 2?

MS. MANCA: I think you want 781, maybe.

MR. FRIEDMAN: That's possible. I'll take your recommendation.

May I have a moment, Your Honor?

THE COURT: Sure.

Q. (By Mr. Friedman) I apologize. This is Exhibit 781. Is this a file that you --

MR. FRIEDMAN: If I could have one moment, Your Honor?

THE COURT: Sure.

MR. FRIEDMAN: Your Honor, Ms. Lye, I would like you to look at Exhibit 812, and we're going to start on the second page.

THE WITNESS: Yep.

MR. FRIEDMAN: I'm sorry, Your Honor. One moment. It is Exhibit 781, and if we could look at page 2.

Q. (By Mr. Friedman) Do you recognize the data in this file?

A. Yes.

Q. Okay. How do you recognize it?

A. This is the customer-offer data that was one of the data sets that was involved in the breach.

Q. Okay.

And if we scan -- do you see names and dates of birth and last four of Social Security numbers there?

A. I do.

Q. And if we scan to the right, can you tell how these individuals -- what city they all live in?

A. Um --

Q. Kind of between the two separate columns of redactions. We can blow it up, if that's helpful.

A. No, I can see it. It looks like they're all in Seattle.

Q. What type of file were the records that we have looked at so far taken from?

A. I didn't see the -- I didn't see the file extension, but I think most of them were .dot dat, like this one. This is CSV, which is comma-separated, but they're, basically, just plain data file.

Q. If we scan further down in this same file to page 5 -- so later records in here -- do you see where the format changes?

A. Yes.

Q. Are these also individuals who reside in Seattle?

A. It looks like it, but there is one Fort Worth there.

Q. Okay. With the exception of that one, Seattle?

A. Yeah.

Q. And is this information from a different Capital One file that has been pulled and put together with information from the first file?

A. It's, actually -- yeah, because one is offered -- well, it's hard to tell. Oh, one is pre-approved and one is ACXIOM, so they do look like two different files that have been concatenated, you know, one put over the other.

Q. So is it fair to say Ms. Thompson has gone into different files --

MR. HAMOUDI: Objection; speculation.

THE COURT: Go ahead and finish your question.

Q. (By Mr. Friedman) is it fair to say that, based on what you see, Ms. Thompson has gone into two different files, taken from Capital One, containing consumer information, and pulled and merged information relating to Seattle residents?

THE COURT: The objection is overruled. You can answer.

A. Based on looking at this now, it appears that information from two different files had been concatenated, one put under the other. That's different than merged, but it does look like two different files have been sort of lifted one over the other.

MR. FRIEDMAN: Thank you, Ms. Lye. I'd ask for the definition of "concatenated," but I'll look that up in the dictionary later. Thank you.

REDIRECT EXAMINATION

BY MR. HAMOUDI:

Q. Ms. Lye, how often have you met with prosecutors in this case?

A. Once.

Q. And when did you meet with them?

A. Monday.

Q. And who was present at that meeting?

A. I don't know, without going and looking at my calendar for all the names.

Q. Was Mr. Friedman present at that meeting, who questioned you?

A. Yes.

Q. And was there an FBI agent present at that meeting?

A. I don't believe so.

Q. Were the lawyers from Capital One present at that meeting?

A. Yes.

Q. And what lawyer? What name is that lawyer?

A. I know that Steve Otero was there.

Q. And who else?

A. I don't know all the names without going and looking at my calendar.

Q. So there were more than one Capital One lawyer present at that meeting, correct?

A. Someone had to drop early in the meeting, so I'm not sure. I don't know.

Q. Okay. Did anybody take notes?

A. I -- I don't know.

Q. Okay. You yourself, as part of that team, missed sensitive data after going through a large amount of data, correct?

A. We did.

Q. Yeah. And how many people were on that team?

A. It varied. The initial team was about 25 people in those first ten days after the breach was discovered, and then we added additional people when we did a second pass through the data in the following few weeks.

Q. And how many hours, approximately, did it take to go through this data?

A. We worked around the clock from when the breach was discovered until the press release was -- until the breach was made public in the press release.

Q. So when was that? Can you give me an approximate time frame?

A. Yeah. So we began work on understanding what had been taken on around the 20th of July, and the announcement was the 29th of July.

Q. And to your knowledge, did Ms. Thompson ever work for Capital One?

A. I don't know.

Q. Okay. Do you know if she has any experience with parquet?

A. I don't know.

Q. And were you aware that -- do you know who Rob Alexander is?

A. I do.

Q. Do you know who the risk committee is?

A. I do.

Q. And what is the risk committee?

A. The risk committee is a senior committee of the executive committee of Capital One. So it is a subcommittee of our executive committee that focuses on properly managing risk for the company.

Q. And is Rob Alexander the chief information officer of Capital One?

A. He is.

Q. And you report to him, correct?

A. I do.

Q. And were you aware that he wrote the risk committee that --

MR. FRIEDMAN: Objection, Your Honor. This is all beyond the scope of cross-examination.

THE COURT: Well, let me hear the question first.

Q. (By Mr. Hamoudi) Were you aware that he wrote the risk committee, in a memorandum on December 13th, 2019, that the Web Application Firewall Role had been granted overly permissive access and that the attacker, Ms. Thompson, was able to access our AWS storage from outside the Capital One network?

THE COURT: Were you aware of that at all, "yes" or "no"?

A. Yes.

THE COURT: I'll overrule the objection.

MR. FRIEDMAN: And I object on grounds of hearsay.

Mr. Alexander is on the witness list if they want to call him.

THE COURT: I overruled the objection. The jury can consider the question and the answer.

Anything else with Ms. Lye?

MR. HAMOUDI: Nothing else.

THE COURT: Mr. Friedman?

MR. FRIEDMAN: Not from the government, Your Honor.

THE COURT: Thank you very much for joining us remotely today. You are excused.

Is your next one a brief one, or should we wait until after lunch?

MR. KLEIN: I think we should wait until after lunch, Your Honor.

THE COURT: Okay.

MR. HAMOUDI: And I'd like to address a brief matter outside the presence of the jury.

THE COURT: Okay. Remember, I talked about flexibility yesterday? Thank you for your flexibility. Come back at 1:10, and we'll try to get started at 1:15. Okay?

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Okay. Thanks. Please be seated. Okay, Mr. Hamoudi?

MR. HAMOUDI: Part of the reason I objected beyond the scope, and what I figured out on direct, is that they're meeting with these witnesses that we've subpoenaed, the government is, and they're interviewing them. And I don't know what they're telling the government during these meetings, and we're certainly entitled, if additional discovery of statements are being produced during these interviews, to get a heads-up, because that's discoverable, even if we subpoenaed these witnesses.

And so I ask the Court just to ask the government that the witnesses that we've identified today, if there was any interviews, that we get a copy of any statements made by these witnesses during these interviews, Your Honor.

THE COURT: Mr. Friedman?

MR. FRIEDMAN: Your Honor, we have interviewed a number of witnesses. The special agent has written 302s that are awaiting signature, and we should be able to provide to the defense.

But I would note that there is nothing exculpatory, particularly in the one of Ms. Lye. It is not *Jencks*. There is no obligation to actually give it. We are giving it because we give all of them. We have no objection if they look at it and say there is something else they want to ask Ms. Lye, but we are going beyond our obligations and will continue doing that.

THE COURT: When do you expect them to be turned over?

MR. FRIEDMAN: The special agent was writing until 3:00 a.m. I assume they're being signed this morning. So over lunchtime.

THE COURT: Great.

MR. HAMOUDI: Thank you, Your Honor.

THE COURT: Okay. So Seth Edgar, Matt Ortiz, you're going to think about Steve Schmidt, Houston Hopkins, Matt Nolan.

MR. KLEIN: Your Honor, I don't know if these 302s cover some of the witnesses we're about to call, but it could affect the decisions we make. So it is a concern for us.

THE COURT: Let's come back at 1:15, and we'll see where you are.

Okay. We'll be adjourned.

(Court in recess 11:52 a.m. to 1:16 p.m.)

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Yes, Mr. Hamoudi?

MR. HAMOUDI: So over the lunch hour, we received seven 302s and notes.

THE COURT: Okay.

MR. HAMOUDI: And the 302s were for Matt Nolan, Rob Alexander, Matt Ortiz, Houston Hopkins, Diane Lye, Seth Edgar, and Steve Schmidt.

Most of the interviews took place on June 13th, one on June 10th, and one on June 12th.

It is a significant amount of information, and these are all of our witnesses, and we --

THE COURT: You're not saying it's not appropriate for the prosecutors to interview the witnesses?

MR. HAMOUDI: No, I'm not saying that.

THE COURT: The FBI has this need to do 302s. Most of the time, you don't even get anything when the prosecutor interviews a witness. But what are you asking for?

MR. HAMOUDI: What I'm asking for this: Is that Ms. Lye testified, and I would have loved the benefit of that 302, because in that 302 she said, "The parquet file," which she spent a length of time testifying to the jury about, "could prove challenging for Ms. Thompson to manipulate." I would have loved to be able to take that 302, show it to her, tell the jury that "you made a statement to a federal agent" that was somewhat inconsistent with what she was saying. And so I would have liked to have that, Your Honor.

And had I not followed up with the questions about attorneys were present and whether she'd been interviewed, I wouldn't have known that there are other interviews that take place, and then we would have marched all these witnesses in, and gotten sandbagged, and --

THE COURT: They gave them to you as soon as they were ready.

MR. HAMOUDI: I think what I would like to do, for her behalf, is that I think we need the afternoon to decide whether we want to call these witnesses. We need to process this information. We need to spend some time to figure out how best next to proceed.

THE COURT: Okay. So I'll bring the jury back, and I'll tell them that we're going to use this afternoon to deal with some legal issues, and I'll ask them to show up tomorrow.

What time do you want, the usual time, or do you need time in the morning to talk to us about whether you're going to call the defendant and whether -- to talk about the other issue?

MR. HAMOUDI: A half hour in the morning, Your Honor.

THE COURT: Okay. So I'll tell the jury to come in at 9:30 or something?

MR. HAMOUDI: Thank you, Your Honor.

THE COURT: Anything, Mr. Friedman?

MR. FRIEDMAN: No, Your Honor, but just for the record and to make clear, in case it is ever an issue later, the reason we interviewed these witnesses is because the defense gave us a witness list with 40 names.

By late Friday, they said, Okay, we're down to these several. We asked Capital One and Amazon whether we could interview them. The interviews, for the most part, took place Sunday -- one Sunday, and four, a very long day, yesterday.

So we've turned this information over incredibly quickly, for which there is no legal obligation anyway.

I just wanted that to be clear for the record.

THE COURT: Okay.

So, Victoria, you can bring the jury in.

THE FOLLOWING PROCEEDINGS WERE HELD
IN THE PRESENCE OF THE JURY:

THE COURT: Flexibility, that's what I'm talking about. So what we're actually going to do here today is, we're going to send you home now, and the lawyers and I are going to work on jury instructions and certain legal matters.

I'd ask you to come in about 9:15 tomorrow, like a half an hour later, and we'll start up at 9:30, and we'll be in a position, I believe, to finish the testimony, and either do instructions and closing arguments tomorrow afternoon, or possibly wait to do those on Thursday morning. But that's where we're headed right now, and we need a little bit of flexibility. So thank you for your patience and understanding.

At the present time, you are excused for the day. Leave your notebooks and pens on your chair, and thank you so much.

THE FOLLOWING PROCEEDINGS WERE HELD
OUTSIDE THE PRESENCE OF THE JURY:

THE COURT: Please be seated.

So you want to take this afternoon to go over the 302s and decide? You could also maybe talk to Ms. Thompson about that issue of whether she's going to testify or not.

Do you want to come back and do any kind of legal arguments this afternoon, or do you want to just take this time and we'll do those tomorrow?

MR. HAMOUDI: We'll take the time, Your Honor. We appreciate it. Thanks.

THE COURT: Okay. Sure.

So tomorrow morning at 9:30, you will tell us what you're going to do. And if you're not going to present those -- some of those witnesses, and you're not going to call the defendant, we'll probably have less than a half day of testimony.

MR. HAMOUDI: Yes, and then we have a pending motion of Mr. Carstens', Your Honor.

THE COURT: I understand.

MR. HAMOUDI: And that's it.

THE COURT: I'm inclined to say we'll take tomorrow -- the rest of tomorrow to finish up the jury instructions and the outstanding issues, and instruct and close on Thursday morning. So that's where -- I see a lot of heads nodding. That will make it better. The more time I give you for closing arguments, the shorter they will be. That's what I'm hoping for.

And, yeah, we got some -- a filing on some of the jury instructions from the government and a response from the defense, and you're not limited to that. We will talk about those tomorrow and make some progress and be ready to go Thursday morning with instructions and arguments. And you want to finish your motion to dismiss at the end of the government's case, too.

MR. HAMOUDI: Yes. I want to make sure I made the record clear, because Ms. Tenney corrected me.

I did not make a general Rule 29 as to all counts, all elements. I want to make sure the record is clear on that.

THE COURT: You did kind of get that in at the end of the argument, but I think you talked about one was fair notice and the other was Constitutional or First Amendment. If you want to say anything more about that.

MR. HAMOUDI: Yeah. I think the First Amendment issue was flagged by the court in one of its orders. The court spoke to there being some First Amendment concerns with the reach of the statute, and so I ask the court to keep that in mind in the context of the arguments I make today on the record.

THE COURT: Okay. And if I need any response from the government, I'll let you know. Okay?

MS. MANCA: Your Honor, I do have one additional matter.

THE COURT: Sure.

MS. MANCA: It is the scope of Dr. Halderman's testimony.

The government was limited, in its examinations, to not rendering an opinion as to whether this conduct actually crossed the line into white hat hacking or black hat hacking, and we would ask that Dr. Halderman's testimony be similarly limited.

THE COURT: I don't even know if they're going to call him, but if they are going to call your expert, the same kind of general rules would apply.

MR. HAMOUDI: Yes, Your Honor.

THE COURT: Okay. Thank you.

All right. We'll be adjourned, and we'll see you tomorrow morning at 9:30.

(Proceedings adjourned at 1:26 p.m.)

CERTIFICATE

I, Nancy L. Bauer, CCR, RPR, Court Reporter for the United States District Court in the Western District of Washington at Seattle, do hereby certify that I was present in court during the foregoing matter and reported said proceedings stenographically.

I further certify that thereafter, I have caused said stenographic notes to be transcribed under my direction and that the foregoing pages are a true and accurate transcription to the best of my ability.

Dated this 14th day of June 2022.

/S/ Nancy L. Bauer

Nancy L. Bauer, CCR, RPR
Official Court Reporter